数理解析研究所講究録
775巻 1992年 141-153

四元数体と正標数の代数幾何

お茶の水大・理　桂　利行 (Toshiyuki Katsura)

§0. 序

k を標数 $p>0$ の代数的閉体とし，E を k 上の楕円曲線とする。E の準同型環を $\mathrm{End}(E)$ とし，$\mathrm{End}^0(E)=\mathrm{End}(E)\otimes_{\mathbb{Z}}\mathbb{Q}$ とおく。E が超特異（定義は §1 参照）ならば，$\mathrm{End}^0(E)$ は，有理数体 $\mathbb{Q}$ 上の判別式 p の definite quaternion division algebra になる。このことによって，多元環の数論と超特異アーベル多様体の代数幾何学に関係がつく。本稿は，その具体的対応をまとめることを目的としている。この対応を用いることによって，超特異アーベル多様体に関する様々な同型類の数の計算を数論的計算に帰着することができ，また，多元環の数論にあらわれる各種の類数に幾何学的な意味を与えることができる。

§1. 偏極アーベル多様体

k を標数 $p>0$ の代数的閉体とし，A を k 上の n 次元アー

ベル多様体とする。A の m 倍写像を $[m]_A$ とかき，写像 $[m]_A$ の核 $\mathrm{Ker}[m]_A$ の被約部分を ${}_mA = \{\mathrm{Ker}[m]_A\}_{red}$ とおく。

$$ {}_mA = \begin{cases} (\mathbb{Z}/m\mathbb{Z})^{\oplus 2n} & \text{if } p \nmid m \\ (\mathbb{Z}/p\mathbb{Z})^{\oplus r} & \text{if } m = p \end{cases} $$

である。ただし，r は，$0 \leq r \leq n$ なる整数である。r を A の p-rank という。ここで，$n=1$ の場合を考え，$A=E$ とおく。

$$ {}_mE = \begin{cases} (\mathbb{Z}/m\mathbb{Z})^{\oplus 2} & \text{if } p \nmid m \\ (\mathbb{Z}/p\mathbb{Z})^{\oplus r} & \text{if } m = p \end{cases} $$

($r=0$ 又は 1) である。$r=0$ のとき，E を超特異楕円曲線という。

$\mathrm{End}^0(E) = \mathrm{End}(E) \otimes_{\mathbb{Z}} \mathbb{Q}$ とおけば，$\mathrm{End}^0(E)$ は $\mathbb{Q}$ 上の多元環であり，次のいずれかになる。

(i) $\mathbb{Q}$，(ii) 虚2次体，

(iii) 判別式 p の $\mathbb{Q}$ 上の *definite quaternion division algebra*.

E の構造層を $\mathcal{O}_E$ とかき，その上の Frobenius 写像を

$$ \begin{array}{cccc} F: & \mathcal{O}_E & \longrightarrow & \mathcal{O}_E \\ & \Psi & & \Psi \\ & f & \longmapsto & f^p \end{array} $$

とする。F は，$H^1(E, \mathcal{O}_E)$ の上の p-線型写像

$$ F^*: H^1(E, \mathcal{O}_E) \longrightarrow H^1(E, \mathcal{O}_E) $$

を引きおこす。このとき，次が成立する。

E：超特異

$\Longleftrightarrow$ $\mathrm{End}^0(E)$ は判別式 p の $\mathbb{Q}$ 上の definite quaternion division algebra

$\Longleftrightarrow$ $F^* = 0$ (零写像)

これを用いて，k 上の超特異楕円曲線の数は，

$$(1) \qquad h = \begin{cases} \dfrac{p-1}{12} + \dfrac{1}{3}\left\{1 - \left(\dfrac{-3}{p}\right)\right\} + \dfrac{1}{4}\left\{1 - \left(\dfrac{-1}{p}\right)\right\} & \text{if } p \geq 5 \\ 1 & \text{if } p = 2 \text{ or } 3 \end{cases}$$

個であることがわかる（Eichler [3], Deuring [2], Igusa [8]）。ここに，$\left(\dfrac{*}{p}\right)$ は Legendre の記号である。E を超特異楕円曲線とするとき，h は，多元環 $\mathrm{End}^0(E)$ の類数に等しくなる。

次の定理は基本的である（Shioda [12] 参照）。

定理 1（Deligne－Ogus－Serre）。

$E, E_1, E_2, \cdots, E_n$ $(n \geq 2)$ を超特異楕円曲線とする。

このとき，

$$E_1 \times E_2 \times \cdots \times E_n \cong E^n \quad (\text{同型})$$

となる。

ここで，超特異楕円曲線 E を 1 つ fix する。

$$B = \mathrm{End}^0(E), \quad \mathcal{O} = \mathrm{End}(E)$$

とおけば，自然に $B \supset \mathcal{O}$ で，$\mathcal{O}$ は B の maximal order となる。B の canonical involution を $\bar{\ }$ とかく。

$$A = E^n, \quad X = E^{n-1} \times \{0\} + E^{n-2} \times \{0\} \times E + \cdots + \{0\} \times E^{n-1}$$

とおく。X は A の principal polarization となる。A 上の任意の因

子Dに対して

$$\begin{array}{cccc} \phi_D : & A & \longrightarrow & A^t = \mathrm{Pic}^0(A) \\ & \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ & x & \longmapsto & T_x^* D - D \end{array}$$

なる準同型をうる。ここに，T_xは，Aの点xによる translation, $\mathrm{Pic}^0(A)$はAの Picard 多様体である。Xは principal polarization 故，ϕ_Xは同型写像となる。これを用いてA上の因子Dに対して，

$$\begin{array}{ccc} \{A\text{上の因子}\} & \longrightarrow & \mathrm{End}(A) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ D & \longmapsto & \phi_X^{-1} \circ \phi_D \end{array}$$

なるアーベル群の準同型写像をうる。A上の因子全体を代数的同値で同値類にわけたものを$NS(A)$とかき，Neron-Severi 群という。これは有限生成アーベル群になる。Aはアーベル多様体であるから，さらに，$NS(A)$は torsion free になる。上記準同型は

$$\begin{array}{ccc} NS(A) & \hookrightarrow & \mathrm{End}(A) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ D\text{の同値類} & \longmapsto & \phi_X^{-1} \circ \phi_D \end{array}$$

なる単射準同型を引きおこす。以下，$NS(A)$の元もDとかく。

$A \cong E^n$より，$\mathrm{End}(A) \cong M_n(\mathcal{O}) \subset M_n(B)$となる。

$M_n(B)$の元は，$K = {}^t\overline{K}$が成立するとき，hermitian であるといわれる。Kを hermitian とするとき，

${}^t x K x \geq 0 \quad \forall x \in B^n$，等号は$x = 0$のときのみ成立

が成立するとき，Kは正定値であるという。

Kをhermitianとするとき，そのHauptnorm をHN(K)とかく(Braun-Koecher [1] 参照)。Bの分解体をLとし

$$M_n(B) \subset M_n(B\otimes L) \cong M_{2n}(L) \qquad (\text{reduced representation})$$

を用いて，Kを$M_{2n}(L)$の元と考えれば

$$\det K = HN(K)^2$$

である。

定理2. $n \geq 2$のとき，次のような対応が存在する。

$$\begin{array}{ccc}
 & & \mathrm{End}(A) \cong M_n(\mathcal{O}) \subset M_n(B) \\
 & & \cup \\
NS(A) & \xleftrightarrow{\text{1対1}} & \{K : \text{hermitian}\} \\
D & \longmapsto & \phi_X^{-1}\circ\phi_D \\
\cup & & \cup \\
\{\text{ample divisor class}\} & \xleftrightarrow{\text{1対1}} & \{K : \text{hermitian},\ \text{正定値}\} \\
\cup & & \cup \\
\{\text{principal polarization}\} & \xleftrightarrow{\text{1対1}} & \{K : \text{hermitian},\ \text{正定値},\ HN(K)=1\}
\end{array}$$

準同型写像 $f: A \longrightarrow A$ に対し，$\mathrm{Pic}^0(A)$ の元の引きもどしとして $f^t: A^t \longrightarrow A^t$ が定義され，次の図式が可換になる:

$$\begin{tikzcd}
A \arrow[r, "\phi_{f^*D}"] \arrow[d, "f"'] & A^t \\
A \arrow[r, "\phi_D"] & A^t \arrow[u, "f^t"']
\end{tikzcd}$$

これを用いて，$\mathrm{End}(A)$の involution を

(2)
$$\begin{array}{ccc} \mathrm{End}(A) & \longrightarrow & \mathrm{End}(A) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ f & \longmapsto & \phi_X^{-1}\circ f^t\circ\phi_X \end{array}$$

と定義する。これは，自然に $\mathrm{End}^0(A)$ の involution を引きおこす (Rosati involution)。また，E の零点を Θ とし，Θ を E の principal polarization と考えれば

$$\begin{array}{ccc} \mathrm{End}(E) & \longrightarrow & \mathrm{End}(E) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ f & \longmapsto & \phi_\Theta^{-1}\circ f^t\circ\phi_\Theta \end{array}$$

なる involution をうる。この involution は，自然に $B=\mathrm{End}^0(E)$ の involution を引きおこすが，これが B の canonical involution にほかならない。このことから (2) から得られる $\mathrm{End}^0(A)\cong M_n(B)$ の Rosati involution は

$$\begin{array}{ccc} M_n(B) & \longrightarrow & M_n(B) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ K & \longmapsto & \overline{K}^t \end{array}$$

なる involution になることがわかる。

$NS(A)\ni D_1, D_2$ に対し

$$\phi_X^{-1}\circ\phi_{D_1}=K_1\ ,\ \phi_X^{-1}\circ\phi_{D_2}=K_2$$

とする。A の自己同型群を $\mathrm{Aut}(A)$ とかく。$\mathrm{Aut}(A)\cong GL_n(\mathcal{O})$ であるから，$\mathrm{Aut}(A)$の元 f は $M_n(B)$の自己同型

(3)
$$\begin{array}{ccc} M_n(B) & \longrightarrow & M_n(B) \\ \rotatebox{90}{$\in$} & & \rotatebox{90}{$\in$} \\ K & \longmapsto & \overline{f}^t\circ K\circ f \end{array}$$

を引きおこす。これを用いて，

(4) $\quad f^*D_1 = D_2$ in $NS(A) \qquad {}^{\exists}f \in Aut(A)$

$$\Longleftrightarrow \quad \bar{f}^t \circ K_1 \circ f = K_2 \qquad {}^{\exists}f \in GL_n(\mathcal{O})$$

となる。

§2. Quaternion hermitian form

本節では，Shimura [13]，Hashimoto-Ibukiyama [5]，Ibukiyama-Katsura-Oort [7] によって，quaternion hermitian form について必要な事柄を整理する。

B を §1 のように，判別式 p の $\mathbb{Q}$ 上の definite quaternion division algebra，$\mathcal{O}$ を B の1つの maximal order とする。B^n を B 上の左ベクトル空間とみる。そのベクトルは横ベクトルを用いて表示する。B^n 上の definite quaternion hermitian form は基底をうまくとれば

(5) $\qquad f(x, y) = \sum_{i=1}^{n} x_i \bar{y}_i \quad ; \quad x = (x_i),\ y = (y_i) \in B^n$

の形になることが知られている (Shimura [13])。$\mathbb{Q}$ の付値 v に対して

$$B_v = B \otimes_{\mathbb{Q}} \mathbb{Q}_v \quad , \quad \mathcal{O}_v = \mathcal{O} \otimes_{\mathbb{Z}} \mathbb{Z}_v$$

とおく。simultitudes の群を

$$G = \{ a \in M_n(B) \mid a\bar{a}^t = \lambda(a) 1_n \quad , \lambda(a) \in \mathbb{Q}^\times \}$$

$$G_v = \{ a \in M_n(B) \mid a\bar{a}^t = \lambda(a) 1_n \quad , \lambda(a) \in \mathbb{Q}_v^\times \}$$

とおく。ただし，1_n は n 次単位行列，$\mathbb{Q}^\times$ (resp. $\mathbb{Q}_v^\times$) は，

$\mathbb{Q}\setminus\{0\}$のなす乗法群 (resp. $\mathbb{Q}_v\setminus\{0\}$ のなす乗法群) である。

$B^n \supset L$ を $\mathbb{Z}$-submodule とする。Lが left $\mathcal{O}$-lattice とは, $\mathbb{Z}$-lattice であって left $\mathcal{O}$-module となるものをいう。B^nの left $\mathcal{O}$-lattices L_1, L_2 に対し

$$L_1 \sim L_2 \ \text{globally equivalent} \Leftrightarrow L_1 a = L_2 \quad {}^\exists a \in G$$

$$L_1 \sim L_2 \ \text{prime } p \text{ で locally equivalent} \Leftrightarrow (L_1 \otimes_{\mathbb{Z}} \mathbb{Z}_p) a = L_2 \otimes_{\mathbb{Z}} \mathbb{Z}_p \quad {}^\exists a \in G_p$$

と定義する。left $\mathcal{O}$-lattice L に対し

$N(L) = f(x, y)$ $(x, y \in L)$ によって生成される両側 $\mathcal{O}$-ideal とおく。これをLの norm という。同じ norm を持つ left $\mathcal{O}$-lattice の中で極大なものを maximal left $\mathcal{O}$-lattice という。

q を素数とするとき, localな状況においても maximal $\mathcal{O}_q$-lattice を同様に定義する。$\mathbb{Q}_q$上の多元環 $B_q = B \otimes \mathbb{Q}_q$ に対しては, 次のようなことが知られている。

1) $B_q = M_2(\mathbb{Q}_q)$ のとき

B_q^n の maximal $\mathcal{O}_q$-lattice は $M_q = \mathcal{O}_q^n$ に equivalent。

2) $B_q =$ division algebra のとき

B_q^n の maximal $\mathcal{O}_q$-lattice は $M_q = \mathcal{O}_q^n$ 又は $N_q = \mathcal{O}_q^n \begin{pmatrix} 1_r & 0 \\ 0 & \pi 1_s \end{pmatrix} \xi$ に equivalent。ただし, $r = [\frac{n}{2}]$, π は $\mathcal{O}_q$ の prime element, $\xi \in GL_n(B_q)$ は $\xi \bar{\xi}^t = \begin{pmatrix} 0 & & 1 \\ & \iddots & \\ 1 & & 0 \end{pmatrix}$ をみたす。

そこで,

$$\mathcal{L}_n(p,1) = \{\text{maximal left } \mathcal{O}\text{-lattice } L \text{ in } B^n \mid L \otimes \mathbb{Z}_q \sim M_q \ \ \forall \text{prime } q\},$$

$$\mathcal{L}_n(1,p) = \left\{\text{maximal left } \mathcal{O}\text{-lattice } L \text{ in } B^n \;\middle|\; \begin{array}{l} L \otimes \mathbb{Z}_q \sim M_q \ \text{ for } q \neq p \\ L \otimes \mathbb{Z}_p \sim N_p \end{array}\right\}$$

とおき，$\mathcal{L}_n(p,1)$ を principal genus，$\mathcal{L}_n(1,p)$ を non-principal genus という。それらの類数を

$H_n = \#(\mathcal{L}_n(p,1)/\text{global equivalence})$ principal genus の類数

$H_n' = \#(\mathcal{L}_n(1,p)/\text{global equivalence})$ non-principal genus の類数

とおく。

$M_n(B)$ の類数が 1 であることから，B^n $(n \geq 2)$ の left $\mathcal{O}$-lattice L は

$$L = \mathcal{O}^n x \qquad {}^\exists x \in GL_n(B)$$

とかけることがわかる。このとき，

$L = \mathcal{O}^n x$，$x \in GL_n(B)$ が $\mathcal{L}_n(p,1)$ に入る

$\iff x\bar{x}^t = mg$ ${}^\exists m \in \mathbb{Q}^\times$, $m > 0$, ${}^\exists g \in GL_n(\mathcal{O})$ s.t. $g = \bar{g}^t$, 正定値

となる。また，(5) でのべたように，g を hermitian で正定値とすれば，$GL_n(B)$ の元 x があって

$$g = x\bar{x}^t$$

とかける。$M_n(B)$ の元 g, h に対して，$GL_n(\mathcal{O})$ の元 a があって $g = \bar{a}^t h a$ となるとき，g と h は同値であるといい，$g \sim h$ とかく ((3) 参照)。このとき

$$\begin{array}{ccc} \mathcal{L}_n(p,1) & \longrightarrow & \{g \in M_n(\mathcal{O}) \mid g : \text{hermitian}, \text{正定値}, HN(g)=1\}/\sim \\ \Psi & & \Psi \\ L=\mathcal{O}^n x & \longmapsto & g \qquad (x\bar{x}^t = mg,\ {}^{\exists}m \in \mathbb{Q}^\times, m>0, g \in GL_n(\mathcal{O})) \end{array}$$

なる全射写像をうるが，この写像は

(6)
$$\begin{array}{ccc} \mathcal{L}_n(p,1)/\text{global equivalence} & \overset{1対1}{\longleftrightarrow} & \{g \in M_n(\mathcal{O}) \mid g : \text{hermitian}, \text{正定値}, HN(g)=1\}/\sim \\ \Psi & & \Psi \\ L=\mathcal{O}^n x & \longmapsto & g \end{array}$$

なる1対1写像を引きおこす。

§3、数論と代数幾何の対応

§1, §2 のように，$A=E^n$ (E：超特異楕円曲線), $\mathcal{O}=\mathrm{End}(E)$, $B=\mathrm{End}^0(E)$ とすれば，自然に $\mathrm{End}\,A \cong M_n(\mathcal{O})$, $\mathrm{End}^0(A) \cong M_n(B)$ となる。$M_n(\mathcal{O})$ の元 K が hermitian で正定値とすれば，A 上の因子 D と $GL_n(B)$ の元 x があって

$$\phi_x^{-1} \circ \phi_D = K = x\bar{x}^t$$

とかける。これを用いれば，定理2と(4), (6) から，$n \geq 2$ のとき，

$$\begin{array}{ccc} \{\text{principal polarization on } A\}/\sim & \overset{1対1}{\longleftrightarrow} & \mathcal{L}(p,1)/\text{global equivalence} \\ \Psi & & \Psi \\ D & \longmapsto & \mathcal{O}^n x \end{array}$$

なる1対1対応を得る。従って，$n \geq 2$ のとき，$A=E^n$ 上の principal polarization の数は，同型をのぞいて，principal genus の類数 H_n に等しいことがわかる。H_n の具体的表示は，$H_1=h$ ((1)参照) であり，H_2 は Hashimoto-Ibukiyama[5], Katsura-Oort[10]，H_3 は Hashimoto[4] で求められている。また，non-principal genus の類数に関しては，$H_1'=h$ であり，H_2' は Hashimoto-Ibukiyama

[5]で計算されている。

標数 $p>0$ とし，アーベル多様体 A がいくつかの超特異楕円曲線の直積に isogenous であるとき，A は超特異であるといわれる。n 次元 principally polarized アーベル多様体のモジュライ空間を $\mathcal{A}_{n,1}$ とするとき，この中で超特異アーベル多様体に対応する点全体 V は，Zariski 閉集合になることが知られている。V の既約成分は上記 genus と関係しており，$n \geq 2$ のとき，既約成分の数は，

n が奇数なら　H_n 個

n が偶数なら　H'_n 個

になることが示される（$n=2$ のとき Ibukiyama-Katsura-Oort [7], Katsura-Oort [9]；$n=3$ のとき Katsura-Oort [10]，n が一般の場合 Li-Oort [11] 参照）。

§4. 付録（2次元の場合）

E を超特異楕円曲線とし，$E_1=E_2=E$ とおく。最後に，$A=E_1\times E_2$ の Néron-Severi 群と多元環の具体的関係を整理しておく。$X=E_1+E_2$，$\mathcal{O}=End(E)$ である。

定理3．次のような1対1対応が存在する。

$$
\begin{array}{ccc}
NS(A) & \xleftrightarrow{1対1} & \left\{ g=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in M_2(\mathcal{O}) \,\middle|\, \alpha,\delta\in\mathbb{Z};\ \beta=\bar{\gamma} \right\} \\
\rotatebox{90}{$\in$}\ D & \longmapsto & \phi_X^{-1}\circ\phi_D\ \rotatebox{90}{$\ni$} \\
\cup & & \cup \\
\{D \mid D>0,\ D^2>0\} & \xleftrightarrow{1対1} & \left\{ g=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \,\middle|\, \alpha,\delta\in\mathbb{Z};\ \beta=\bar{\gamma},\ \alpha>0,\ \delta>0,\ \det g>0 \right\}
\end{array}
$$

この対応において，

$$\phi_X^{-1}\circ\phi_D=\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}$$

とすれば，

$$(D\cdot E_1)=\alpha\ ,\quad (D\cdot E_2)=\delta$$

$$D^2=2\det g$$

となる。

References

[1] H. Braun and M. Koecher, Jordan Algebren, Springer-Verlag, 1966.

[2] M. Deuring, Die Typen der Multiplikatorenringe elliptischer Funktionenkörper, Abh. Math. Sem. Univ. Hamburg 14 (1941), 197-272.

[3] M. Eichler, Über die Idealklassenzahl total definiter Quaternionenalgebren, Math. Z. 43 (1938), 102-109.

[4] K. Hashimoto, Class numbers of positive definite ternary quaternion hermitian forms, Proc. J. Acad., 59 (1983), 490-493.

[5] K. Hashimoto and T. Ibukiyama, On class number of positive definite binary quaternion hermitian forms (I), J. Fac. Sci. Univ. Tokyo Sect IA, 27 (1980), 549-601, (II) ibid. 28 (1981), 695-699, (III) ibid. 30 (1983), 393-401.

[6] T. Ibukiyama, On automorphism groups of positive definite binary quaterion hermitian lattices and new mass formula, to appear.

[7] T. Ibukiyama, T. Katsura and F. Oort, Supersingular curves of genus two and class numbers, Compositio Math. 57 (1986), 127-152.

[8] J. Igusa, Class number of a definite quaternion with prime discriminant, Proc. Nat. Acad. Sci. U.S.A. 44 (1958), 312-314.

[9] T. Katsura and F. Oort, Families of supersingular abelian surfaces, Compositio Math., 62 (1987), 107-167.

[10] T. Katsura and F. Oort, Supersingular abelian varieties of dimension two or three and class numbers, Adv. Stud. in Pure Math. 10, 1987, Algebraic Geometry, Sendai 1985, pp.253-281.

[11] K. Li and F. Oort, Moduli of supersingular abelian varieties, in preparation.

[12] T. Shioda, Supersingular K3 surfaces, Lecture Notes in Math. 732, Berlin-Heidelberg-New York, Springer (1979), 564-591.

[13] G. Shimura, Arithmetic of alternating forms and quaternion hermitian forms, J. Math. Soc. Japan 15 (1963), 33-65.